UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,366	10/14/2003	William Joseph Eakin	10018596-1	4386

22879 7590 01/26/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
D AGOSTA, STEPHEN M	

ART UNIT	PAPER NUMBER
2683	

DATE MAILED: 01/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/685,366	EAKIN, WILLIAM JOSEPH	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2683	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, see Appeal Brief, filed 1-4-2006, with respect to the rejection(s) of claim(s) 1-32 under USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection (see below).

1. The examiner discussed the case with Mr. Phil Lyran on 1-6-2006. It is the applicant's position that the claims recite using the appliance ID (eg. phone number) of a device to log-in to a network. The examiner disagrees with this position since the claims do not specifically state that this is the ONLY indicia that is provided during the log-in process.

For example, claim 1 recites "..receiving a private database access request...including ***at least an*** appliance ID...comparing the appliance ID...and communicating the information from the private database to the wireless device".

First and foremost, claim 1 states that AT LEAST an appliance ID is provided. Hence, anything else can be provided and compared since additional items are not ruled out. The claim does not state that the process ONLY uses the appliance ID for comparing/logging-in, it only states that it is used. Hence, it does not specifically rule out the use of any other means (eg. log-in name, password, etc.) during the process.

The examiner has applied new art to show that various data can be provided and compared to log-on a user to a network/server. The applicant is invited to amend the claims to state that ONLY the appliance ID can used for log-in purposes. The examiner further notes that the amendment should also state that NO OTHER factors are used for login/security purposes (to rule out passwords, logins, etc.).

2. As an additional note to Claim 1, the examiner notes that it appears the remote user has already logged into the database server (or at least does not rule out that the user has already logged into the server) since the claim does not recite how or when the user accessed the network. It only states that a request is made. Is a network logon required? Is a network logon not required? Did the user already logon to

the network and provide a password such that only the appliance ID is now used for communications? These points should be defined in the claim.

3. Claims 12 and 15 are similar to claim 1 in that they state the appliance ID is used. It does not state that ONLY the appliance ID is used to perform the log-in. Hence other data such as sender's hardware/IP address, logon name and password can be used as well.

4. Claims 19, 22, 24 and 27 are again similar to claims 1/12/15 since they do not state that only the appliance ID is used. They state that wireless device can communicate with the private database "only when the appliance ID corresponds to a security indicia" but it does not rule out that this is the ONLY data that is checked/verified. Hence the user can include their hardware/IP address, logon and password.

5. The examiner has provided new art for the independent claims, each of which describes using ***at least*** the phone number to authenticate/identify the user.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 to 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison US 2002/0069355 and further in view of Rezvani et al. US 2002/0077077 **and** (Shimada **or** Wilber **or** Khouri **or** Obouchi **or** Ronen **or** Yamazaki).

As per **claims 1, 12, 19, 22 and 24-25 and 27**, Garrison teaches a method for communicating information from a private database to a wireless communication device (abstract, figure 1 and Para#33 teaches wireless communications), comprising:

receiving a private database access request from the wireless communication device, (figure 4a-b and Para#42 teaches Username/Password which uniquely ID's the user/device) ;

comparing the password with a security indicia, the security indicia associated with the wireless communication device (figure 3 teaches a Password table #55 which is checked as does figures 4a-b), and

communicating the information from the private database to the wireless communication device when the appliance ID corresponds to the security indicia (figures 4a-b teaches authenticating the user and sending the data if the user is verified) **but is silent on** the private database access request including ***at least*** an appliance identification (ID) that uniquely identifies the wireless communication device and comparing the appliance ID with security indicia.

Garrison teaches authenticating a user via username and password, as pointed out by the primary examiner above. Garrison discloses use of many different communications networks (see Para#33) and one skilled understands that this would encompass use of the Internet. Hence the client's device/computer would use TCP/IP addressing which would inherently uniquely identify the appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

Shimada teaches using the telephone number of a device to register said device and connect to a network (abstract. Note that figure 1 shows the Internet being used).

Wilber teaches:

"If a carrier is detected at 236, a signal is sent to the local computer 52 which requests or prompts the local computer 52 to provide a **caller ID *(eg. phone number)*** and a password at step 242. The caller ID and password are verified at step 244, and if found appropriate a file transfer is executed at step 246" (C5, L58-62)

Khouri teaches:

In another embodiment, a database may be established to maintain specific caller priorities 66. ***Specific callers may be***

identified by the caller's telephone number 60 or the caller may be asked to provide an access code or user ID.

In this embodiment, the database may identify the caller in order to establish their priority within the queue using their telephone number, password, or user ID. (C6, L54-65)

Obouchi teaches:

FIG. 3 is a graphical table illustrating exemplary contents in a collection of registered sentences for individual. Private information items that identify the user, such as the ID, name, telephone number and password of that user, are preferably appended to the collection of registered sentences for that individual. (C5, L56-61)

Ronen teaches:

Specifically, in these embodiments, before they are sent to the telephone company, the user's telephone number and a password known only to the user and to the telephone company, are encrypted with a public encryption key that is associated with only the telephone company. After authenticating the user by confirming the association between the decrypted telephone number and the password provided by the user, the ISP begins to provide the requested information and/or interactive services to the user. (C2, L62 to C3, L5)

Yamazaki teaches::

To make this possible, the pager uses a caller's telephone number as a password. (Abstract)

With further regard to claims 19 and 22 and 30-31, Garrison teaches use of password authentication and RF transmissions while Rezvani teaches use of an ESN number which reads on applicant's use of term "multiple use" (see claim 2 below as well) and transmitter/processor (see figure 1).

With further regard to claim 24, Garrison teaches a computer system/program executed on client and server (figures 2-3) with software logic shown in figures 4a-b)

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the private database access request including at least an appliance identification (ID) that uniquely identifies the wireless communication device

and comparing the appliance ID with security indicia, to provide added security checking of both login/password and device ID.

As per **claims 2 and 13,** Garrison teaches claim 1/12, **but is silent on** wherein the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device.

Rezvani teaches authenticating a user via an ESN number of a cellular phone (Para #4 and 6) which reads on the applicant's use of the term "multiple-use identification" ("Appliance ID 210 is a serial number, phone number, security code, or other suitable unique identifier, of the cell phone 102 that uniquely identifies cell phone 102. Accordingly, the appliance ID 210 is referred to herein as a multiple-use unique identifier since the appliance ID 2 1 0 uniquely identifies the appliance and identifies the appliance as an authorized device to embodiments of the private database wireless access system").

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device, to provide means for an ID to have multiple uses (ie. used as a phone number, security check, etc.)

As per **claims 3, 14 and 26,** Garrison teaches claim 2/13/25 **but is silent on** wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device.

Rezvani teaches authenticating a user via an ESN number of a cellular phone (Para #4 and 6) which reads on using the telephone number/MIN of the phone since both uniquely identify the user and can be used interchangeably.

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device, to provide for associating a user to their phone for security purposes (eg. that one user will use that one phone).

As per **claim 4,** Garrison teaches claim 1 **but is silent on** wherein the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device.

Rezvani teaches transmitting data/header to a remote system that includes transmission of information including identification information (Para#66 and figure 4, #254/#258).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device, to provide means for transmitting the appliance ID in the overhead of a message header.

As per **claim 5,** Garrison teaches claim 1, wherein communicating further comprises transmitting the information radio frequency (RF) signal to the wireless communication device.

As per **claim 6,** Garrison teaches claim 1, wherein receiving the private database access request further comprises receiving information selecting one of a plurality of different private databases wherein the selected private database is communicated to the wireless communication device when the appliance ID corresponds to the security indicia (figures 4a-b teach the user being verified and then having access to databases, figure 1, 20a-d).

As per **claims 7 and 15-16,** Garrison teaches claim 1/13, further comprising;

receiving a second private database access request from a second wireless communication device (Para #3 teaches authorized access by users), the second private database access request including at least a password generated by a user (Para#42);

comparing the received password with a security code, the security code uniqtlely associated with the user (Para#42); and

but is silent on associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device.

Garrison teaches authenticating a user via username and password, as pointed out by the primary examiner above. Garrison discloses use of many different communications networks (see Para#33) and one skilled understands that this would encompass use of the Internet. Hence the client's device/computer would use TCP/IP addressing which would inherently uniquely identify the appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device, to provide means for the system to support access by a plurality of users based on their device ID and/or login/password.

As per **claim 8,** Garrison teaches claim 7, **but is silent on** further comprising saving the second unique appliance ID as the second security indicia uniquely associated with the second wireless communication device.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). The ESN is stored until the phone roams away and/or is shutoff. Hence the second appliance ID would be stored by the network/database until the user terminates contact.

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it saves the second unique appliance ID as the second security indicia uniquely associated with the second wireless communication device, to

provide means for keeping a user and user's device ID on record for security tracking/verification purposes.

As per **claim 9,** Garrison teaches claim 7, further comprising:

receiving a subsequent private database access request from the second wireless communication device (figures 4a-b) **but is silent on** the subsequent private database access request including at least the second unique appliance ID,

comparing the second unique appliance ID with the second security indicia, and

communicating the private database to the second wireless communication device when the second unique appliance ID corresponds to the second security indicia.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the subsequent private database access request including at least the second unique appliance ID, AND comparing the second unique appliance ID with the second security indicia, AND communicating the private database to the second wireless communication device when the second unique appliance ID corresponds to the second security indicia, to provide means for supporting a plurality of users who can be verified before accessing the database.

As per **claim 10,** Garrison teaches claim 1, further comprising:

uniquely associating a plurality of unique passwords with a plurality of unique passwords (figure 3, #55 and Para#42)

wherein one password uniquely identifies one of a plurality of wireless communication devices and wherein each of the security indicia are uniquely associated with one of a plurality of private databases (figure 1 shows multiple databases),

receiving the private database access request from one of the plurality of wireless communication devices, the private database access request comprising at least the password of the transmitting wireless communication device and an access request to a selected private database selected from the plurality of private databases (figures 4a-b),

comparing the password of the transmitting wireless communication device with the plurality of unique security indicia (figures 4a-b); and

communicating the selected private database to the transmitting wireless communication device when the password corresponds to the security indicia of the selected private database (figures 4a-b) **but is silent on**

use of appliance IDs which are check/verified to initiate access to database(s).

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses appliance IDs which are check/verified to initiate access to database(s), to provide means for multiple levels of security verification to include device ID, login, password, etc..

As per **claims 11 and 18,** Garrison teaches claim 1/12, further comprising receiving a communication from the wireless communication device that prevents association of the password with the security indicia so that communicating the private database to the wireless communication device is prevented (Para#42 and figures 4a-b) **but is silent on** use of an appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses appliance IDs which are check/verified to initiate access to database(s), to provide means for multiple levels of security verification to include device ID, login, password, etc..

As per **claim 17 and 29,** Garrison teaches claim 12/27 **but is silent on** further comprising:

selecting a portion of the received private database using a browser, and

displaying the selected portion of the received private database on a display residing on the wireless communication device using the browser.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access and view a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134). Note Para#108 specifically teaches "..client device 22 may include, for example, an Internet browser application that may be used to access web pages via communications network 16".

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that selecting a portion of the received private database using a browser, AND displaying the selected portion of the received private database on a display residing on the wireless communication device using the browser, to provide support for Internet access.

As per **claim 20,** Garrison teaches claim 19, further comprising a memory configured to store the received private database (figure 2 is the client device which comprises a memory, #22).

As per **claim 21,** Garrison teaches claim 19, further comprising:

a display (figure 2, #29) **but is silent on** a browser configured to display the received private database on the display.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access and view a (remote) database via communication means (Para#'s 108-111, 113 teaches celluar phone access, 121, 122 and 134). Note Para#108 specifically teaches "..client device 22 may include, for example, an Internet browser application that may be used to access web pages via communications network 16".

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses a browser configured to display the received private database on the display, to provide means for access via the Internet.

As per **claim 23,** Garrison teaches claim 22 further comprising security code corresponding to a user associated with the private database, so that when the received ID is not initially associated with the security indicia, a password provided by the user of the remote wireless communication device causes the multiple-use unique ID to be associated with the security indicia when the password corresponds to the security code (Para#42 teaches use of login/password which is associated with the user's device).

As per **claim 28**, Garrison teaches claim 27 further comprising transmitting via both Internet and RF communications, the information from the remote database to the PWCD (figure 1 and Para #33 shows connections from the user to the remote database. Since Garrison teaches both wired/wireless technology, one skilled understands that the mobile user will send an RF message which will eventually be connected to a wired/Internet connection that connects to the database server).

Claim 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison/Rezvani/(Shimada **or** Wilber **or** Khouri **or** Obouchi **or** Ronen **or** Yamazaki). and further in view of Schneider et al. US 6,178,505.

As per **claim 32**, Garrison teaches claim 27 comprising authenticating, without a user of the PWCD entering a password, whether the PWCD is authorized to access the information stored in a remote database.

Schneider teaches authentication, albeit poor, via just an IP Address:

> As is clear from the above list of identification information, the degree to which a firewall can trust identification information to authenticate a user depends on the kind of identification information. For example, the IP address in a packet can be changed by anyone who can intercept the packet; consequently, the firewall can put little trust in it and authentication by means of the IP address is said to have a very low trust level. On the other hand, when the identification information comes from a token, the firewall can give the identification a much higher trust level, since the token would fail to identify the user only if it had come into someone else's possession. (C3, L16-27)

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that a password is not required, to provide means for different levels of security.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 571-272-7862. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bill Trost can be reached on 571-272-7872. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

WILLIAM TROST
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600

STEVE M. D'AGOSTA
PRIMARY EXAMINER

1-17-06